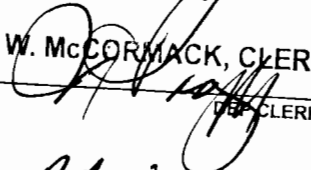


IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF ARKANSAS

FILED
U.S. DISTRICT COURT
EASTERN DISTRICT ARKANSAS

JAN 16 2015

JAMES W. McCORMACK, CLERK
By:  DEPT. CLERK

ALCOA COMMUNITY FEDERAL
CREDIT UNION, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

THE HOME DEPOT, INC.,

Defendant.

CASE NO: *4:15cv39-BRW*

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

This case assigned to District Judge *Wilson*
and to Magistrate Judge *Kearney*

Plaintiff, Alcoa Community Federal Credit Union (“Alcoa Credit Union” or “Plaintiff”), individually and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to it and on information and belief as to all other matters, by and through counsel, brings this Class Action Complaint against The Home Depot, Inc. (“Home Depot” or the “Defendant”).

INTRODUCTION

1. Beginning as early as April 1, 2014, Home Depot’s security networks were hacked compromising the financial and personal data of approximately 56 million Home Depot customers as a result of Home Depot’s acts and omissions (the “Security Breach”). Plaintiff brings this class action on its own and on behalf of all other similarly situated financial institutions (“Class Members”) seeking damages resulting from Home Depot’s unreasonable conduct, misrepresentations, and negligence.

2. Home Depot did not detect the Security Breach of its payment card systems until it was brought to its attention on September 2, 2014 by its banking partners and law enforcement, *nearly five months after the breach began*. The breach compromised customer data, including names, account numbers, card expiration dates and card verification values.¹

3. Home Depot failed to use adequate security measures to protect customer data including having weak passwords and a lack of lockout security procedures. These failures allowed hackers to gain access to the Home Depot security systems and proceed with the theft of millions of consumer data information.

4. Even after learning of the Security Breach on September 2nd, Home Depot waited until September 8th to acknowledge the Security Breach and that over fifty million customers' personal and financial information had been stolen. It was security blogger, Brian Krebs, who first broke the news of the breach to the public on September 2nd. Thereafter, Home Depot began an investigation into the data breach in conjunction with private security firms and the United States Secret Service.

5. Several months later, on November 6, 2014, Home Depot announced that approximately 53 million email addresses had been stolen *in addition* to the payment card information previously announced as stolen in September.²

6. As a result of the Security Breach, the Plaintiff and Class Members that issue credit and debit cards have suffered millions of dollars in damages. Plaintiff and Class Members suffered losses resulting from Home Depot's data breach related to a) reimbursement of fraudulent charges or reversal of customer charges; b) lost interest in transaction fees, including lost interchange fees; and c) administrative expenses and overhead charges associated with

¹ <https://corporate.homedepot.com/MediaCenter/Documents/FAQs.pdf>.

² <https://corporate.homedepot.com/MediaCenter/Documents/FAQs.pdf>.

monitoring and preventing fraud, as well as purchasing and mailing new payment cards to their customers.

7. Home Depot has publicly acknowledged that it is responsible for the Security Breach.

JURISDICTION AND VENUE

8. This court has jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d), in that (a) the class (as defined below) has more than 100 class members; (b) the amount at issue exceeds five million dollars (\$5,000,000.00), exclusive of interest and costs; and (c) greater than two thirds of the Class Members are citizens of states other than Arkansas.

9. This court has personal jurisdiction over Home Depot because the company operates retail locations nationwide including within the State of Arkansas.

10. Venue is proper in this Court under 28 U.S.C. § 1391(b)(1), (b)(2) & (c)(2) because Home Depot conducts substantial business in this district and is subject to personal jurisdiction in this district. Finally, venue is proper in this district because a substantial part of the events or omissions giving rise to the claim occurred in this district.

11. The causes of action alleged in this complaint are timely brought within the applicable limitations period.

PARTIES

12. Plaintiff Alcoa Community Federal Credit Union is a not-for-profit financial cooperative located in Benton, Arkansas.

13. Defendant Home Depot is incorporated in Delaware and does business throughout the United States, including Arkansas. Home Depot's headquarters and principal place of business are located in Atlanta, Georgia.

FACTUAL ALLEGATIONS

A. Home Depot Did Not Reasonably Protect Consumers' Sensitive Financial and Personal Information

14. On September 2, 2014 Home Depot became aware that a breach had occurred on its payment card system. Specifically, computer hackers installed malware to access the point-of-sale ("POS") systems at Home Depot retail stores throughout the United States and Canada. The breach compromised customer data, including names, account numbers, card expiration dates and card verification values going back as far as April 1, 2014.³

15. Home Depot failed to use adequate security measures to protect customer data including having weak passwords and a lack of lockout security procedures. These failures allowed hackers to gain access to the Home Depot security systems and proceed with the theft of millions of customer data information. Lockout security procedures prevent entry into a system after several failed password attempts. By failing to have these security measures in place, hackers were able to try many combinations of usernames and passwords in their successful attempt to gain access to Home Depot's security network and POS systems.

16. After gaining entry into Home Depot's security system, the hackers used "RAM scraper" malware to gain access to Home Depot's customers' financial and personal information. This type of malware has been used to attack POS terminals since at least 2011. Home Depot failed to detect this malware on its systems for over five months, permitting the hackers to continue to steal customers' financial information. Had Home Depot been more diligent in its efforts to monitor its systems for malware, this theft could have been prevented.

³ <https://corporate.homedepot.com/MediaCenter/Documents/FAQs.pdf>.

17. Cards stolen from Home Depot shoppers first turned up for sale on Rescator.cc in early September, the same underground cybercrime shop that sold millions of cards stolen in the Target security breach. “There are signs that the perpetrators of this apparent breach may be the same group of Russian and Ukrainian hackers responsible for the data breaches at Target, Sally Beauty and P.F. Chang’s, among others.”⁴

18. Home Depot’s failure to maintain adequate security, including failure to properly monitor their systems, enabled the Security Breach resulting in the theft and subsequent fraudulent transactions on customers’ credit and debit cards.

19. Further, on November 6, 2014, Home Depot announced that approximately 53 million email addresses had been stolen *in addition* to the payment card information previously announced as stolen in September. The failure of Home Depot to protect not only its customers’ financial information but also their private email addresses compounded the Security Breach.

20. As the world’s largest home improvement retailer, Home Depot operates 1,977 stores in the United States and 180 in Canada. That is about 400 more than Target had when it was compromised. Target’s breach went on for three weeks before the company learned about it, while the attack at Home Depot went unnoticed for as long as five months. According to a New York Times article, one estimate of illegal purchases as a result of the Security Breach reaches as high as \$3 billion dollars.⁵

21. Not only did Home Depot fail to detect the intrusion into its security systems for five months, but Home Depot’s in-store payment system was not even set up to encrypt

⁴ <http://krebsonsecurity.com/tag/home-depot-databreach/>.

⁵ http://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html?_r=0.

customers' credit- and debit-card data. This deficit in its defenses gave potential hackers a wider window to exploit, according to interviews with former members of Home Depot's security team.

22. Five former Home Depot staffers describe "a work environment in which employee turnover, outdated software, and a stated preference for 'C-level security'" (as opposed to A-level or B-level) hampered the team's effectiveness."⁶

23. One Home Depot employee even warned friends and family to use cash at Home Depot stores rather than credit cards due to the inadequate security measures.⁷

24. Despite Home Depot's knowledge of similar breaches at other major retailers including Target less than a year earlier and knowledge of weaknesses in its own system, Home Depot failed to adopt adequate security measures that would have defended against this attack. Home Depot's own employees began raising alarms about the lax security at Home Depot as early as 2008.⁸

25. A "health check" on Home Depot's information systems performed by Symantec two months before the breach identified out-of-date malware-detection systems, according to one former manager. "The former information security managers say that when they attempted to make improvements to Home Depot's security systems, they were at times turned down by its technology executives, including information security chief Jeff Mitchell. Three former

⁶ <http://www.businessweek.com/articles/2014-09-12/home-depot-didnt-encrypt-credit-card-data-former-workers-say>.

⁷ http://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html?_r=0.

⁸ http://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html?_r=0.

information security managers also say that Home Depot was using out-of-date antivirus software for its point-of-sales systems.”⁹

26. Symantec’s Endpoint Protection 11, which Home Depot was employing throughout the breach, was released in 2007. Symantec unveiled version 12 in 2011, saying in a news release that the “threat landscape has changed significantly” and that the newer product would protect against the “explosion in malware scope and complexity.”¹⁰ Despite the availability of newer and better software, Home Depot stayed with Endpoint Protection 11.

27. The financial and personal data stolen from Home Depot customers and now for sale on Rescator.cc includes both the information needed to fabricate counterfeit cards as well as the legitimate cardholder’s full name and the city, state and ZIP of the Home Depot store from which the card was stolen. “This is especially helpful for fraudsters since most Home Depot transactions are likely to occur in the same or nearby ZIP code as the cardholder. The ZIP code data of the store is important because it allows the bad guys to quickly and more accurately locate the Social Security number and date of birth of cardholders using criminal services in the underground that sell this information.”¹¹

28. Social Security numbers and dates of birth are particularly important as most banks in the United States allow customers to change their PINs with a telephone call, using an automated call-in system known as a Voice Response Unit (VRU). A large number of these VRU systems allow the caller to change their PIN provided they pass three out of five security checks, including: the 3-digit code printed on the back of the debit card; the card’s expiration

⁹ *Id.*

¹⁰ *Id.*

¹¹ <http://krebsonsecurity.com/2014/09/in-wake-of-confirmed-breach-at-home-depot-banks-see-spike-in-pin-debit-card-fraud/>.

date; the customer's date of birth; the last four digits of the customer's Social Security number. Once the hacker has obtained this information, he can change the pin number on a debit card, and then use the card to withdraw cash at any ATM.

29. While, Home Depot was quick to assure customers and banks that no debit card PIN data was compromised by the breach, the theft of the other personal and financial data of consumers may have led to the same result of debit cards being breached for cash transactions. Multiple financial institutions reported to KrebsOnSecurity a steep increase in fraudulent ATM withdrawals on customer accounts after the Security Breach.¹²

30. Home Depot's failure to safeguard customer information, failure to maintain adequate security measures, and failure to detect intrusion for over five months has resulted in millions of dollars in damages for Plaintiff and the Class Members. Plaintiff and Class Members suffered losses resulting from Home Depot's data breach related to a) reimbursement of fraudulent charges or reversal of customer charges; b) lost interest in transaction fees, including lost interchange fees; and c) administrative expenses and overhead charges associated with monitoring and preventing fraud, as well as purchasing and mailing new payment cards to their customers.

31. Compounding the damages to Plaintiffs, Home Depot directed its customers to their financial institutions, the Class Members, for answers regarding the data breach; thus, only adding to the heavy call volumes and customer service representatives needed at these institutions, further increasing administrative expenses.¹³

¹² <http://krebsonsecurity.com/2014/09/in-wake-of-confirmed-breach-at-home-depot-banks-see-spike-in-pin-debit-card-fraud/>

¹³ <https://corporate.homedepot.com/MediaCenter/Documents/FAQs.pdf>.

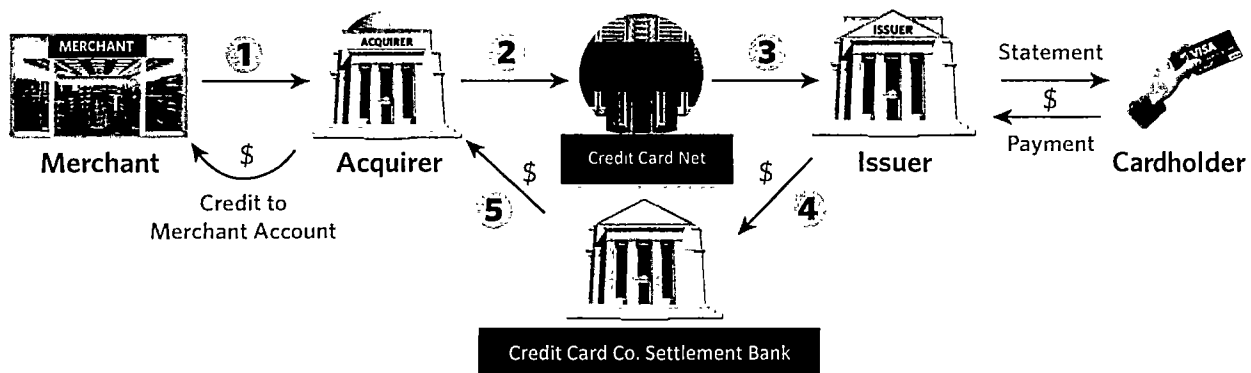
B. Home Depot Had a Duty to Act with Reasonable Care to Protect Consumers' Sensitive Financial and Personal Information

32. There are several parties to a typical credit or debit card transaction. The transaction begins when a consumer uses his or her debit or credit card at the point of sale system of the merchant (in this case Home Depot). The point of sale system then transmits the card information (data encoded on the magnetic strip) to the acquiring bank.

33. The merchant contracts with this acquiring bank to process its debit and credit card transactions. The acquiring bank then transmits the card information and a request message to the processor (generally, the credit card company such as Visa, MasterCard, American Express). The credit card company routes the request to the issuing bank for review and approval.

34. The issuing bank is the financial institution, which issued the credit or debit card directly to the consumer. Plaintiff and Class Members are issuing banks. If the transaction is approved, the issuing bank will post the transaction to the consumer's credit or debit card account.

35. The chart below graphically depicts an example of such a credit transaction:



36. Each credit card company has its own rules and regulations, but all companies monitor their networks for potential fraudulent activity. If the credit card company detects fraudulent activity, it will notify the issuing bank. Likewise, if a participant in the credit card company's network detects fraudulent activity it is required to report such activity to the credit card company.

37. Home Depot, like all retailers who accept credit and debit cards, are required to comply with the regulations for each of the credit card companies' cards, which it accepts at its retail locations (generally, "Card Operating Regulations").

38. Home Depot and other parties in the credit card networks also have a duty to follow the Payment Card Industry Data Security Standard ("PCI Standard").

39. The PCI Standard is an industry standard for large retail institutions that accept credit and debit card transactions. The PCI Standard requires the following:

- i. Build and Maintain a Secure Network
 - install and maintain a firewall configuration to protect data
 - do not use vendor supplied defaults for system passwords and other security parameters
- ii. Protect Cardholder Data
 - protect stored data
 - encrypt transmission of cardholder data and sensitive information across public networks
- iii. Maintainable a Vulnerability Management Program
 - use and regularly update antivirus software
 - develop and maintain secure systems and applications
- iv. Implement Strong Access Control Measures
 - restrict access to data by business need to know
 - assign unique ID to each person with computer access
 - restrict physical access to cardholder data

- v. Regularly Monitor and Test Networks
 - track and monitor all access to network resources and cardholder data
 - regularly test security systems and processes
- vi. Maintain an Information Security Policy
 - maintain a policy that addresses information security

40. The PCI Standard is intended to:

Build and maintain a secure network; protect cardholder data; ensure the maintenance of vulnerability management programs; implement strong access control measures; regularly monitor and test networks; and ensure the maintenance of information security policies.¹⁴

41. Home Depot failed to meet the PCI Standard by, among other things, failing to maintain an adequately secure network, failing to protect cardholder data, and failing to regularly monitor its network for intrusions.

42. Home Depot knew or should have known that the RAM scraper malware was a real threat, as it had been used since 2011 for data breaches including in attacks against Target, Sally Beauty, P.F. Chang's, Neiman Marcus, Michaels Stores, and Supervalu.

43. Home Depot knew that its malware detection systems were out of date, that is software provider, Symantec, had released a newer, more effective, and better system two years before the Security Breach, which was set to replace the outdated seven-year old program used by Home Depot; yet, Home Depot chose not to update its systems, leaving itself and its customers vulnerable to attack.

44. Home Depot knew or should have known that failing to protect customer's financial and personal data would cause harm to financial institutions, such as the Plaintiff and other Class Members. Home Depot repeatedly assured customers that customers would not be

¹⁴ https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf.

responsible for any fraudulent charges knowing that Plaintiff and other Class Members would be required to cover those fraudulent charges resulting from the Security Breach.¹⁵

45. Home Depot owed Plaintiff and other Class Members a duty of care, which it patently breached.

46. The acts and omissions of Home Depot caused and will continue to cause damage to Plaintiff and other Class Members in the form of a) reimbursements of fraudulent charges or reversal of customer charges; b) lost interest in transaction fees, including lost interchange fees; and c) administrative expenses and overhead charges associated with monitoring and preventing fraud, as well as purchasing and mailing new payment cards to their customers. These costs are ongoing as additional fraudulent charges are discovered.

C. Financial Institutions Have Been Directly Harmed By Home Depot's Unreasonable Behavior And Will Continue To Be Harmed

47. Plaintiff and Class Members suffered losses directly resulting from Home Depot's data breach related to a) reimbursement of fraudulent charges or reversal of customer charges; b) lost interest in transaction fees, including lost interchange fees; and c) administrative expenses and overhead charges associated with monitoring and preventing fraud, as well as purchasing and mailing new payment cards to their customers.

48. As a result of Home Depot's unreasonable acts and omissions, Plaintiff and Class Members, to protect their customers and avoid fraud losses, cancelled payment cards they had issued. Plaintiff and Class Members reissued cards with new account numbers and magnetic strip information to customers incurring administrative, overhead and mailing costs.

¹⁵ <https://corporate.homedepot.com/MediaCenter/Documents/FAQs.pdf>.

49. As a result of Home Depot's failure to safeguard customer information, Plaintiff and Class Members have been forced to expend time and resources on added fraud monitoring, reissuance of debit and credit cards, additional personnel to respond to customer inquiries and issues related to the Security Breach, and have had further expenses related to fraudulent charges and lost interchange fees.

50. Home Depot's negligent maintenance of its security systems and failure to take necessary precautions to protect its customers' personal and financial data has resulted in damages to the Plaintiff and Class Members.

CLASS ACTION ALLEGATIONS

51. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(2) and (b)(3), Plaintiff brings this action on behalf of a class defined as follows:

All banks, credit unions, and other financial institutions in the United States that, as a result of the Home Depot Security Breach, have suffered damages and/or harm with respect to the disclosure of personal and financial information of their customers from approximately April 1, 2014 through and until the effects of the Defendant's conduct ceases.

52. Plaintiff is a member of the Class that it seeks to represent. Excluded from the Class are Defendant; any parent, subsidiary, or affiliate of Defendant or any employees, officers or directors of Defendant; legal representatives, successors, or assigns of Defendant; and any justice, judge, or magistrate judge of the United States who may hear the case, and all persons related to any such judicial officer, as defined in 28 U.S.C. § 455(b).

53. This action is brought and may properly be maintained as a class-action pursuant to 28 U.S.C. § 1332(d). This action satisfies the procedural requirements set forth in Fed. R. Civ. P. 23.

54. There are substantial questions of law and fact common to the Class. The questions include, but are not limited to, the following:

- a. Whether Defendant failed to provide adequate security and/or protection for its computer systems containing customers' financial and personal data;
- b. Whether the conduct of Defendant resulted in the unauthorized breach of its computer systems containing customers' financial and personal data;
- c. Whether the Defendant was negligent in collecting, storing, and/or transmitting the sensitive financial data of its customers;
- d. Whether Defendant knew or should have known of the vulnerability of its computer systems to breach;
- e. Whether Defendant knew or should have known of the risks to financial institutions inherent in failing to protect such financial and personal information;
- f. The nature and extent of damages and injunctive relief to which Plaintiff and the Class Members are entitled; and,
- g. Whether Plaintiff and the Class Members should be awarded attorneys' fees and costs.

55. Plaintiff's claims are typical of the claims of the Class Members. Plaintiff and all Class Members were damaged by the same unreasonable conduct of Defendant.

56. Plaintiff will fairly and adequately protect and represent the interests of the Class. The interests of the Plaintiff are coincident with, and not antagonistic to, those of the Class.

57. Plaintiff has retained counsel competent and experienced in the prosecution of complex class-action litigation.

58. Members of the Class are so numerous that joinder is impracticable. Plaintiff believes that there are hundreds, if not thousands of Class Members. Further, the Class is readily identifiable from information and records maintained by Defendant.

59. Questions of law and fact common to the members of the Class predominate over questions that may affect only individual Class Members because Defendants have acted on grounds generally applicable to the entire Class, thereby determining damages with respect to the Class as a whole is appropriate. Such generally applicable conduct is inherent in Defendant's unreasonable conduct.

60. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated persons or entities to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweighs potential difficulties in management of this class action.

61. Plaintiff knows of no special difficulty to be encountered in the maintenance of this action that would preclude its maintenance as a class action.

COUNT ONE
Negligence

62. Plaintiff incorporates by reference each of the preceding paragraphs as if fully set forth herein.

63. Defendant had a continuing duty to Plaintiff, Class Members, and Class Members' customers, the millions of U.S. consumers who shop at Defendant's stores, to use and exercise reasonable and due care in obtaining, retaining, and safeguarding the personal and financial information of Plaintiff, other Class Members, and Class Members' customers.

64. Defendant owed a duty to Plaintiff and other Class Members to take reasonable measures to provide adequate security to protect the personal and financial information of Plaintiff, other Class Members, and Class Members' customers. Because Defendant came into possession of the personal and financial information of Plaintiff's and other Class Members' customers, Defendant had a duty to exercise reasonable care in safeguarding and protecting such information from being accessed, compromised and/or stolen by third parties.

65. Defendant breached its duties, allowed an unlawful, catastrophic intrusion into its computer system, failed to protect against such an intrusion, and allowed personal and financial information to be accessed, compromised and/or stolen by third parties.

66. Defendant had a duty to employ adequate and reasonable procedures for the safeguarding of the financial and personal information of Plaintiff's and other Class Members' customers.

67. Defendant, through its acts and/or omissions, unlawfully breached its duty to Plaintiff and other Class Members by failing to maintain adequate, reasonable procedures designed to protect against unauthorized access and/or theft of financial and personal information

68. Defendant knew or should have known with the reasonable exercise of care of the risk inherent in retaining such information and the importance of providing adequate security.

69. But for Defendant's negligent and wrongful breach of its duties owed to Plaintiff and other Class Members, financial and personal information would not have been accessed, compromised, and/or stolen.

70. As a direct and proximate result of Defendant's unreasonable conduct, Plaintiff and other Class Members have suffered substantial damages, which they seek to recover.

71. Further, Defendant's actions were patently unreasonable with respect to the rights of the Plaintiff and other Class Members. Defendant knew or should have known, in light of the surrounding circumstances that its negligence would naturally and probably result in damages to Plaintiff and other Class Members. Substantial, ongoing damages did result for Plaintiff and other Class Members. Thus, punitive damages should be awarded to deter the actions of Defendant and others who might engage in similar action or conduct.

COUNT TWO

Negligent Misrepresentation

72. Plaintiff incorporates by reference each of the preceding paragraphs as if fully set forth herein.

73. Millions of Defendant's customers made purchases at Defendant's stores with credit and debit cards issued by Plaintiff and other Class Members. By participating in credit and debit card systems, Defendant falsely represented that it would comply with the Card Operating Regulations and would safeguard customer data to induce banks to act as issuing banks, such as Plaintiff and other Class Members, and provide their customers with credit and debit cards for use at Home Depot stores.

74. Defendant's compliance with Card Operating Regulations and safeguarding of customer data were material facts upon which Plaintiff and other Class Members relied.

75. Defendant knew or should have known that it was not in compliance with the Card Operating Regulations and was not safeguarding customer data. Defendant represented that it was safeguarding customer data, which included a representation that it would maintain adequate security measures and would maintain the confidentiality of such information.

76. Plaintiff and other Class Members agreed to act as issuing banks for the debit and credit transactions, reasonably expecting that Defendant would comply with the Card Operating Regulations and would safeguard customer data. Plaintiff and other Class Members relied upon and acted in reliance upon Defendant's representations.

77. Plaintiff and other Class Members justifiably relied upon the false representations made by Home Depot regarding the security and confidentiality of the credit and debit card information.

78. Defendant knew or should have known that Plaintiff and other Class Members would rely on Defendant's representations regarding the security of financial and personal information.

79. As a proximate result of the Defendant's negligent misrepresentation, Plaintiff and other Class Members have suffered actual damages in an amount to be proven at trial.

80. Defendant's actions were unreasonable with respect to the rights of the Plaintiff and other Class Members. Defendant knew or ought to have known, in light of the surrounding circumstances that its negligent misrepresentation would naturally and probably result in damages to Plaintiff and other Class Members. Defendant continued its wrongful conduct with

disregard for the consequences. Punitive damages should be awarded to deter the actions of Defendant and others who might engage in similar action or conduct.

COUNT THREE
Negligence *Per Se*

81. Plaintiff incorporates by reference each of the preceding paragraphs as if fully set forth herein.

82. Home Depot has a duty to protect and keep confidential the personal and financial information of cardholders that conduct transactions at Home Depot Stores under the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801.

83. Defendant violated the Gramm-Leach-Bliley Act by failing to adhere to the Card Operating Regulations and PCI Standards, as well as failing to protect its customers' personal and financial information.

84. Defendant's violation of the Card Operating Regulations and PCI Standards is negligence *per se*.

85. Plaintiff and other Class Members have suffered damages as a result of Defendant's negligence *per se*.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of itself and the Class, respectfully requests that the Court:

- A. Determine that this action may be maintained as a class action pursuant to Federal Rule of Civil Procedure 23(a), (b)(2) and (b)(3), and direct that reasonable notice of this action, as provided by Federal Rule of Civil Procedure 23(c)(2), be given to the Class, and declare Plaintiff the Representative of the Class;

- B. Enter judgment against the Defendant and in favor of Plaintiff and the Class;
- C. Adjudge and decree under Fed. R. Civ. P. 57 and 18 U.S.C. § 2201(a) the acts alleged herein by Defendant were negligent behavior, negligent misrepresentations, and negligence *per se*;
- D. Award compensatory damages to Plaintiff and the Class in an amount to be determined at trial;
- E. Award punitive damages, including treble damages, in an appropriate amount;
- F. Enter an injunction permanently barring continuation of the conduct complained of herein; and
- G. Award Plaintiff and the Class the costs incurred in this action together with reasonable attorneys' fees and expenses, including any necessary expert fees as well as pre-judgment and post-judgment interest;
- H. Grant such other and further relief as is necessary to correct for the effects of the Defendant's unlawful conduct and as the Court deems just and proper.

JURY TRIAL DEMAND

Plaintiff, on behalf of itself and others similarly situated, hereby requests a jury trial, pursuant to Federal Rule of Civil Procedure 38, on any and all claims so triable.

DATED: January 16, 2015

Respectfully submitted

A handwritten signature in black ink, appearing to read "Mike Roberts", written over a horizontal line.

Mike Roberts, AR Bar #90125
ROBERTS LAW FIRM, P.A.
20 Rahling Circle
P.O. Box 241790
Little Rock, AR 72223-1790
(501) 821-5575 (p)
(501) 821-4474 (f)
mikeroberts@robertslawfirm.us

COUNSEL FOR PLAINTIFF